网络安全技术

刘振

上海交通大学 计算机科学与工程系

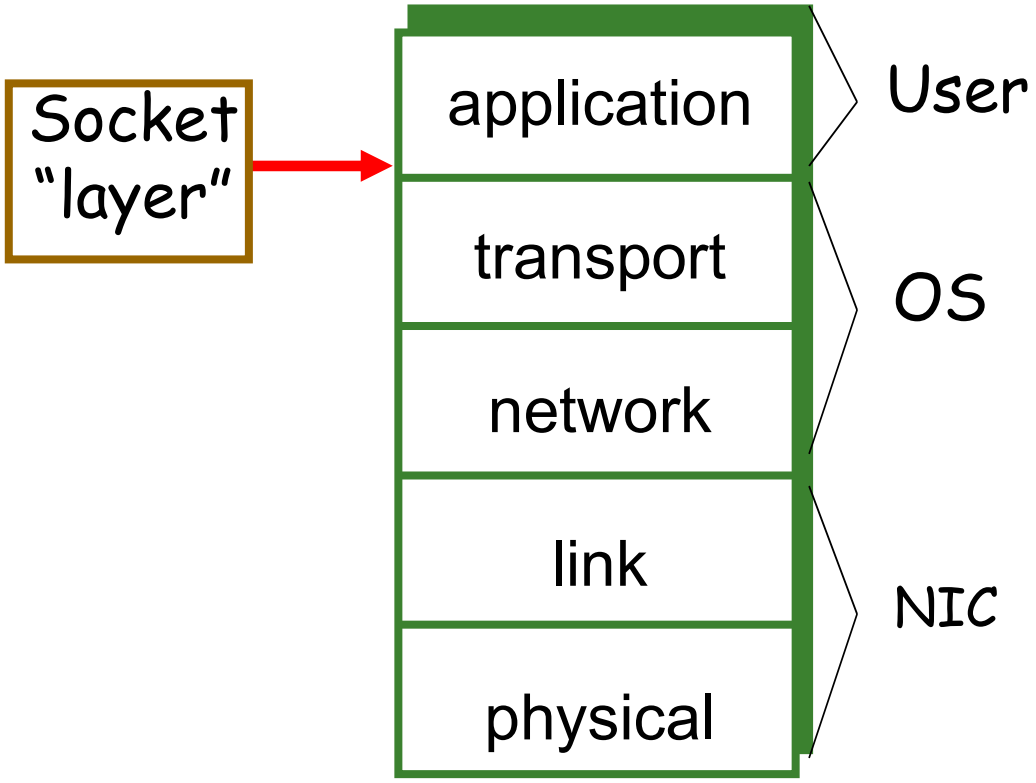
电信群楼3-509

liuzhen@sjtu.edu.cn

Secure Socket Layer

Socket layer

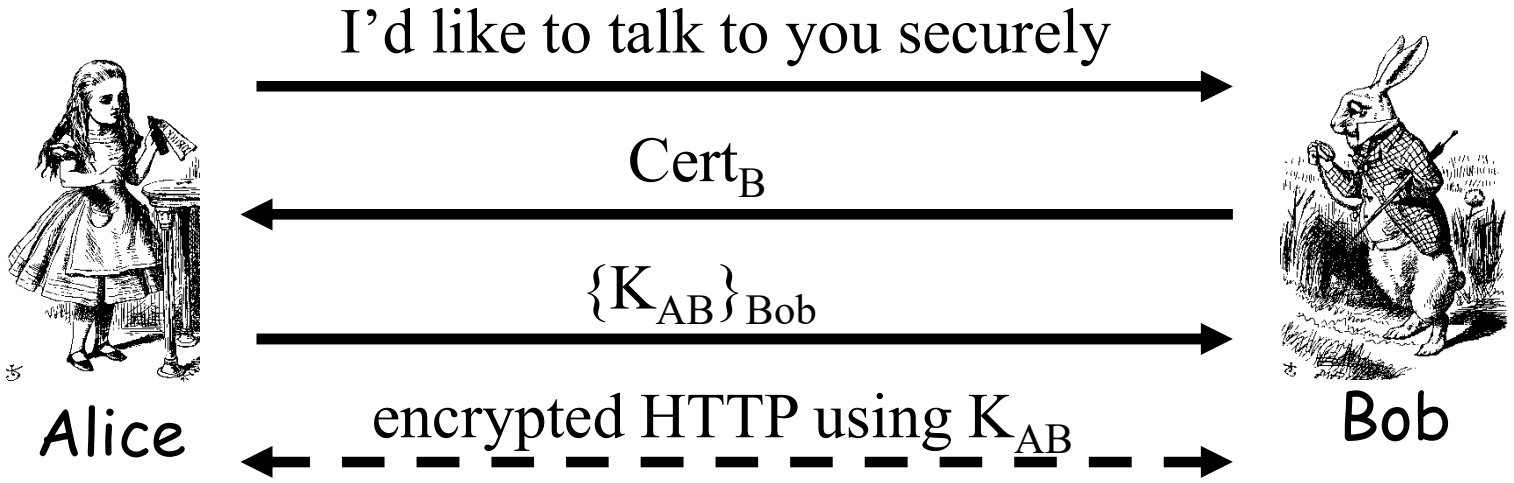
- "Socket layer" lives between application and transport layers
- SSL usually lies between HTTP and TCP



What is SSL?

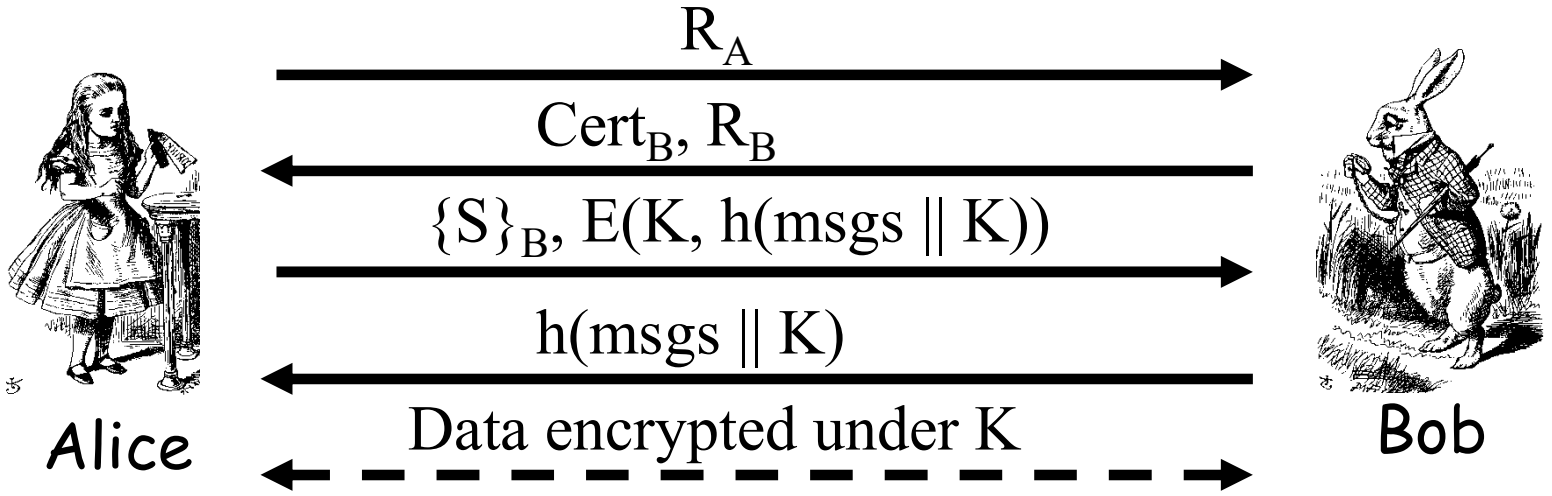
- SSL is the protocol used for most secure transactions over the Internet
- For example, if you want to buy a book at amazon.com…
  - You want to be sure that you are dealing with Amazon (**one-way authentication**)
  - Your credit card information must be protected in transit (**data confidentiality**)
  - As long as you have money, Amazon doesn't care who you are (**authentication need not to be mutual**)

Simple SSL-like Protocol



- Is Alice sure she's talking to Bob?
- Achieve Data Confentiality?
- Forward secrecy?

Simplified SSL Protocol



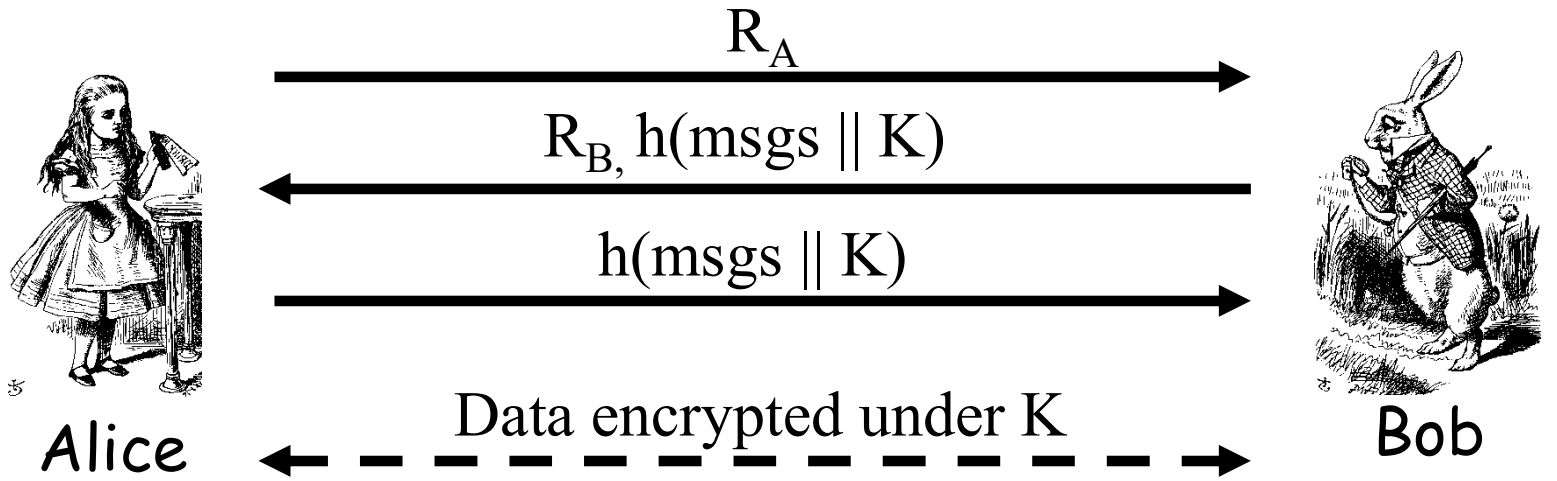
- S is **randomly chosen by Alice**
- $K = h(S,R_A,R_B)$
- msgs = all previous messages

- Forward secrecy?

SSL Sessions vs Connections

- SSL designed for use with HTTP 1.0
- HTTP 1.0 usually opens multiple simultaneous (parallel) **connections**
- SSL session establishment is costly
  - Due to public key operations
- **SSL has an efficient protocol for opening new connections given an existing session**

SSL Connection



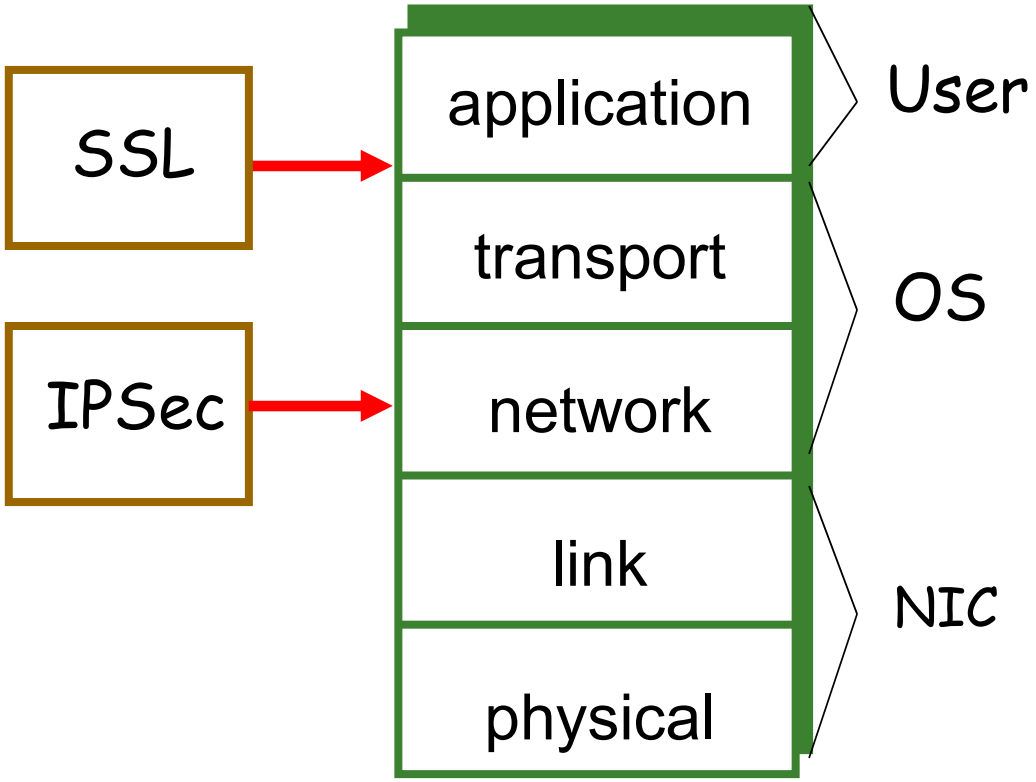
- Assuming SSL **session** exists
- So S is already known to Alice and Bob
- Again, $K = h(S,R_A,R_B)$

- **No public key operations!** (relies on known S)

IPSec

IPSec and SSL

- IPSec lives at the network layer
- IPSec is transparent to applications



IKE and ESP/AH

- Two parts to discuss
  1. Establish a session key – IKE (Internet Key Exchange)
  2. How a secure channel works – ESP or AH (Encapsulating Security Payload, Authentication Header)

- In SSL, it also has these two parts
  - We have only discussed the first part – establishing a session key
  - We didn't discuss how the secure channel works

IKE

- IKE has 2 phases
  - Phase 1 — master session key setup
  - Phase 2 — ESP and/or AH key setup
- Phase 1 is comparable to SSL session
- Phase 2 is comparable to SSL connection

- In this course, we don’t cover Phase 2

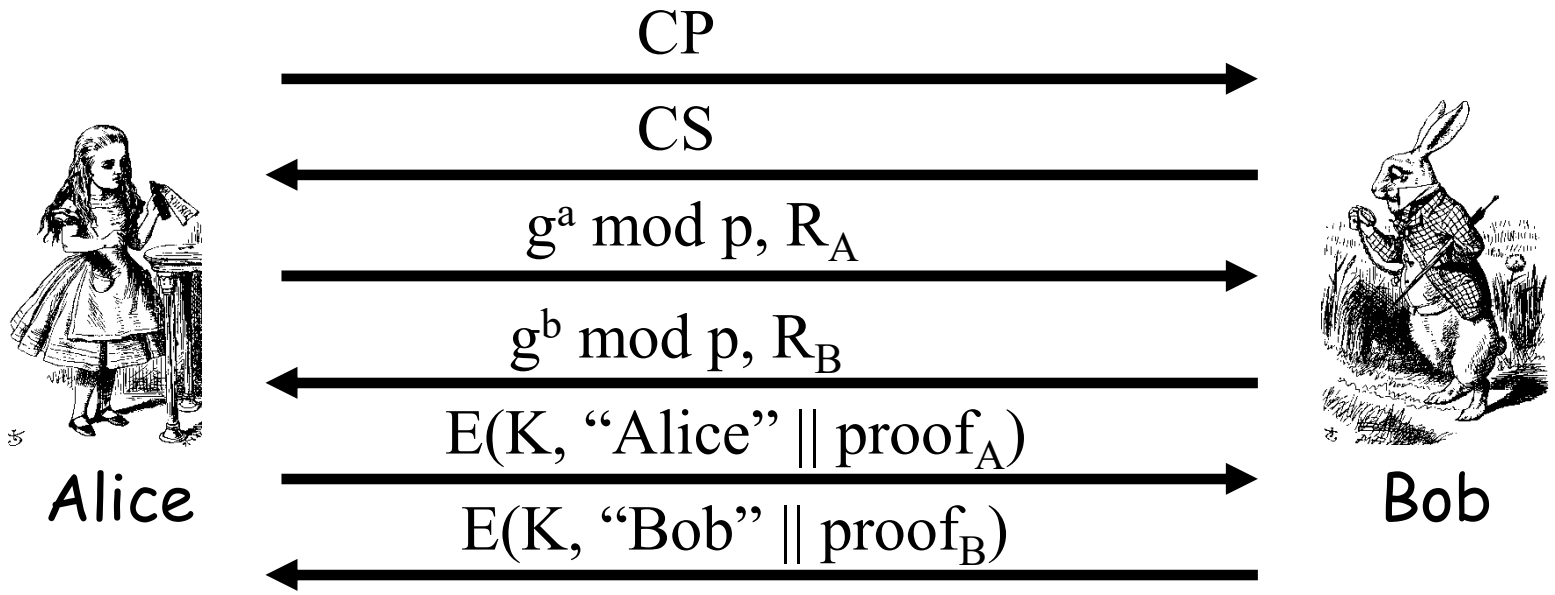
IKE Phase 1

- Three ways to run phase 1
  - Public key encryption based
  - Signature based
  - Symmetric key based
- For each of these, there are two different “modes” to choose from
  - Main mode
  - Aggressive mode
- **There are 6 variants of IKE Phase 1!**
- Evidence that IPSec is over-engineered?

IKE Phase 1

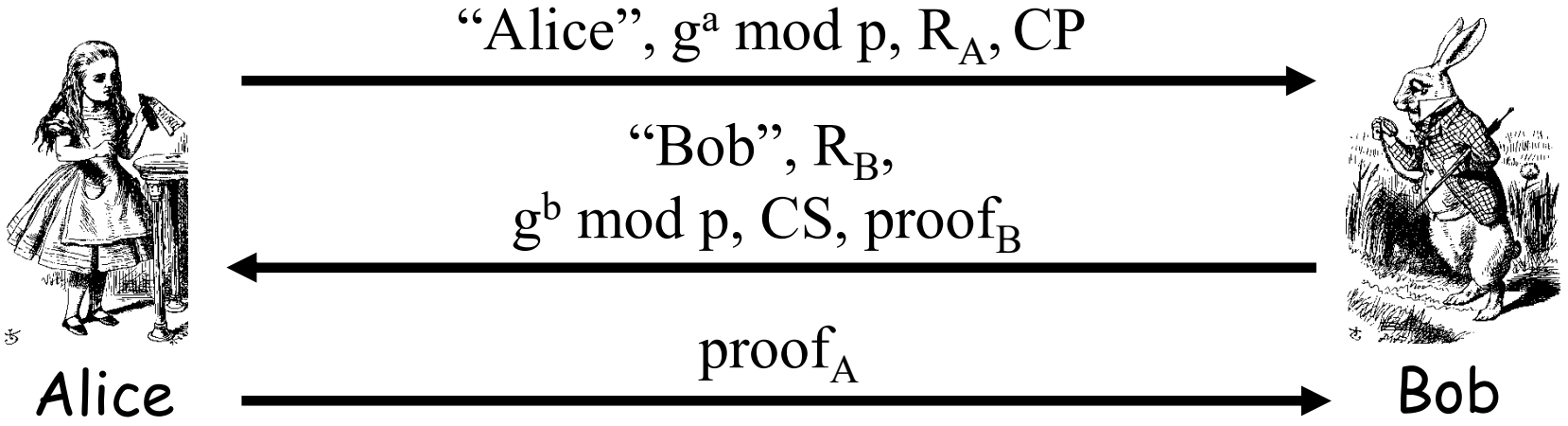
- According to the IKE specification,
  - Main mode **MUST** be implemented
  - Aggressive mode **SHOULD** be implemented
  - In other words, if aggressive mode is not implemented, “you should feel guilty about it”

IKE Phase 1: Signature Based (Main Mode)



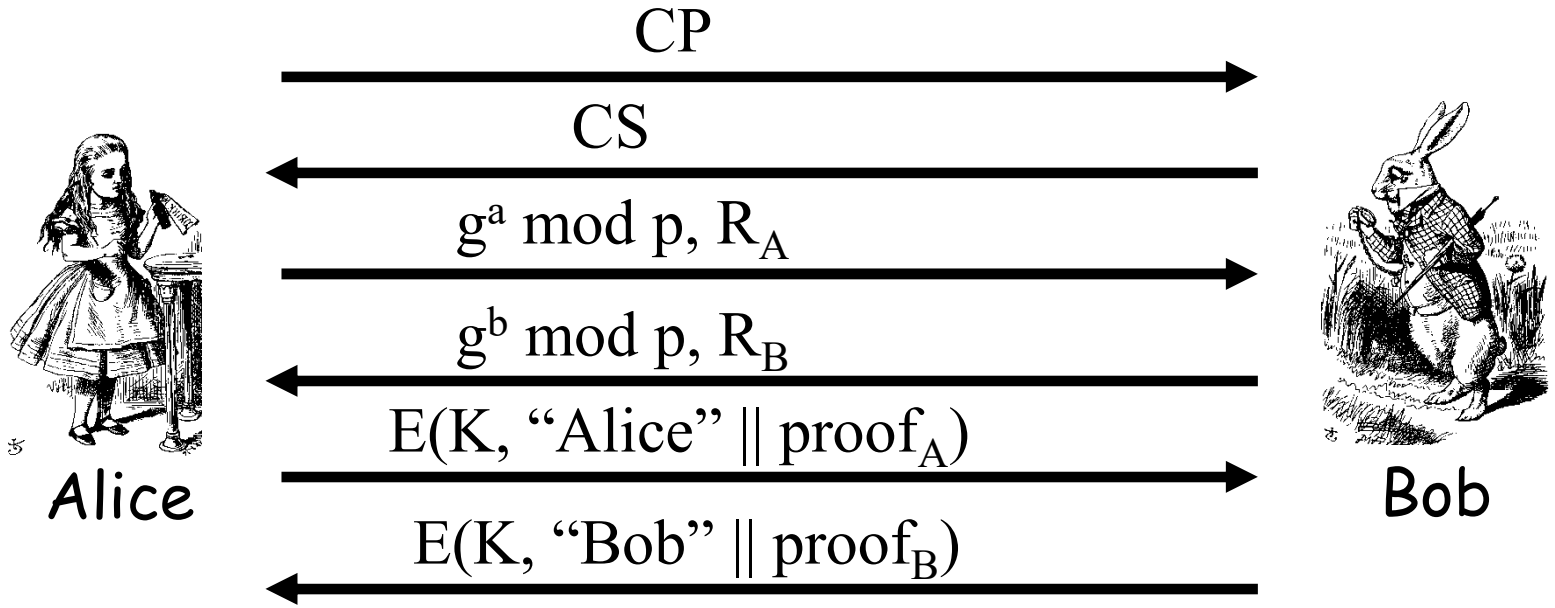
- CP = crypto proposed, CS = crypto selected
- K = h(g^{ab} mod p, R_A, R_B)
- SKEYID = h(R_A, R_B, g^{ab} mod p)
- $proof_A$ = [h(SKEYID, g^a mod p, g^b mod p, CP, "Alice")]$_{Alice}$

IKE Phase 1: Signature Based (Aggressive Mode)



- Main difference from main mode
  - Not trying to protect identities
  - Cannot negotiate g or p

IKE Phase 1: Symmetric Key Based (Main Mode)

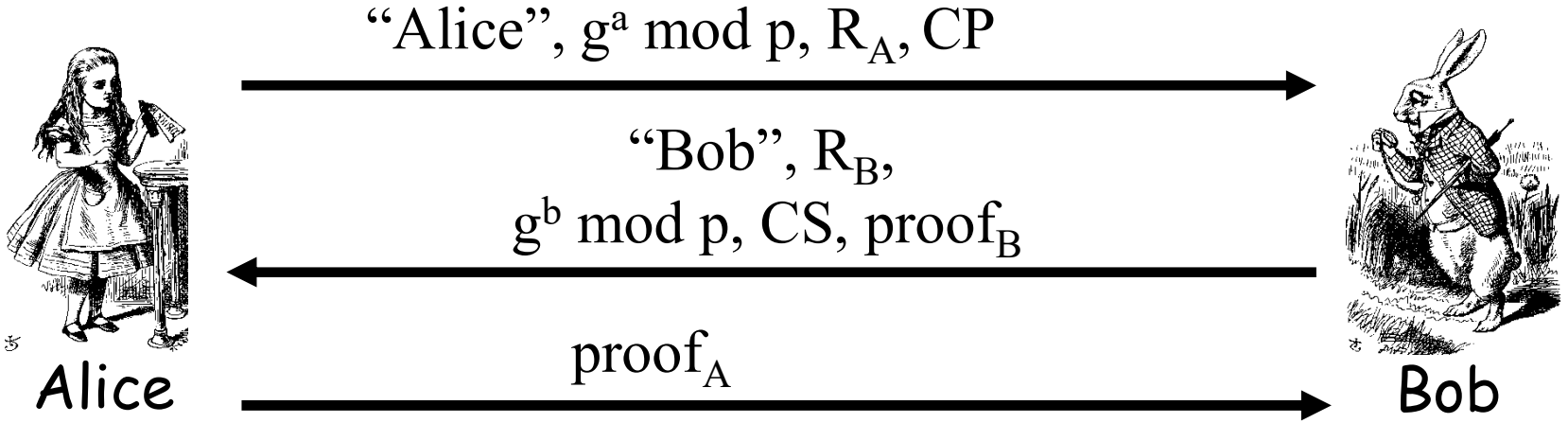


- K_{AB} = symmetric key shared in advance
- $K = h(g^{ab} \bmod p, R_A, R_B, K_{AB})$
- $SKEYID = h(K, g^{ab} \bmod p)$
- $proof_A = h(SKEYID, g^a \bmod p, g^b \bmod p, CP, \text{"Alice"})$

Problems with Symmetric Key Based (Main Mode)

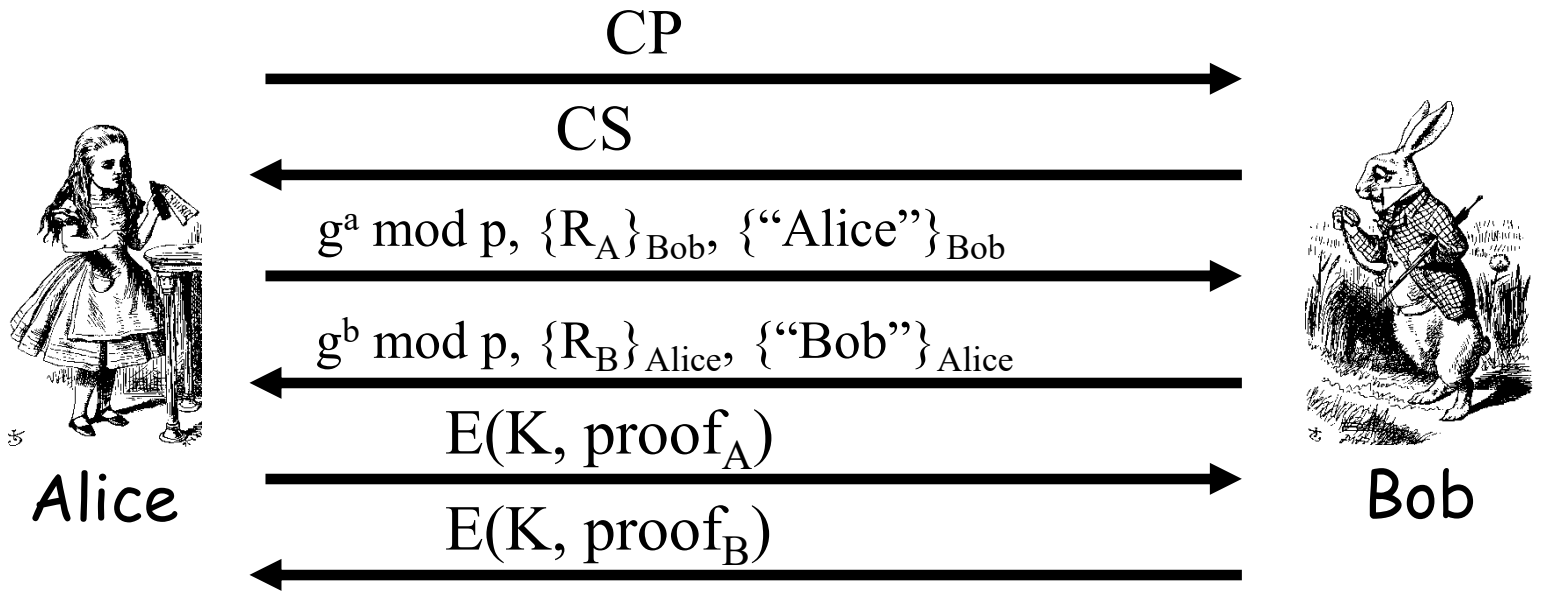
- Catch
  - Alice sends her ID in message 5
  - Alice's ID encrypted with K
  - To find K Bob must know K_{AB}
  - To get K_{AB} Bob must know he's talking to Alice!
- Result: **Alice's ID must be IP address!**

IKE Phase 1: Symmetric Key Based (Aggressive Mode)



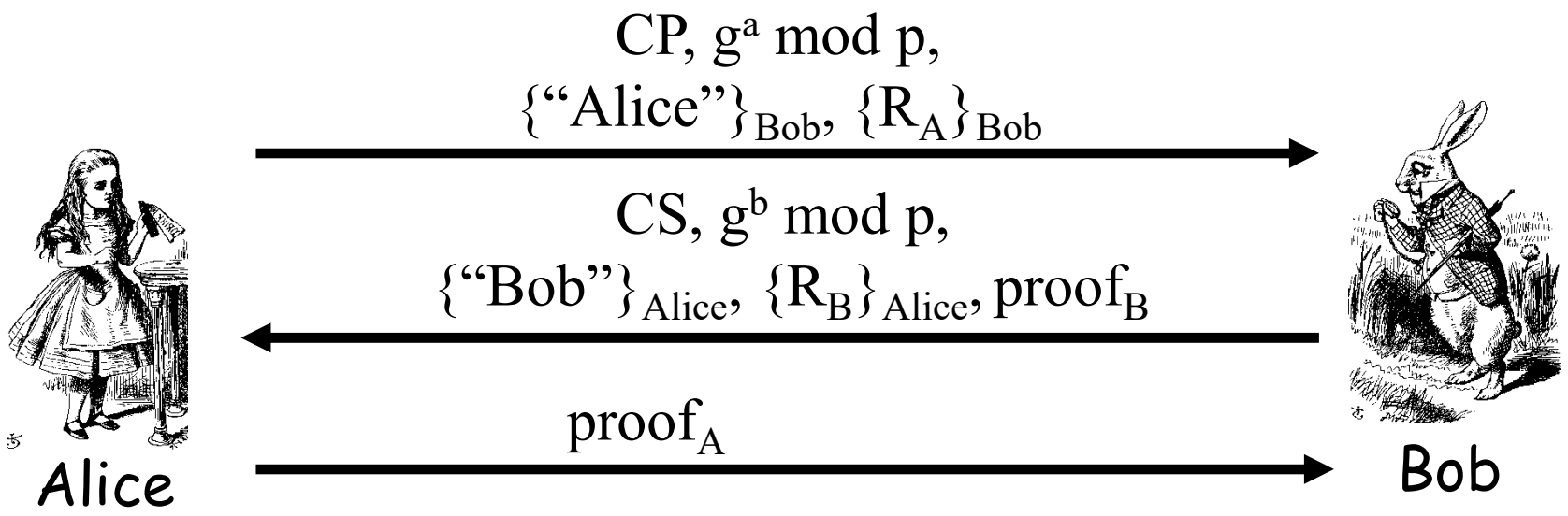
- Same format as digital signature aggressive mode
- Not trying to hide identities…
- As a result, does **not** have problems of main mode

IKE Phase 1: Public Key Encryption Based (Main Mode)



- $K = h(g^{ab} \bmod p, R_A, R_B)$
- $SKEYID = h(R_A, R_B, g^{ab} \bmod p)$
- $proof_A = h(SKEYID, g^a \bmod p, g^b \bmod p, CP, \text{“Alice”})$

IKE Phase 1: Public Key Encryption Based (Aggressive Mode)

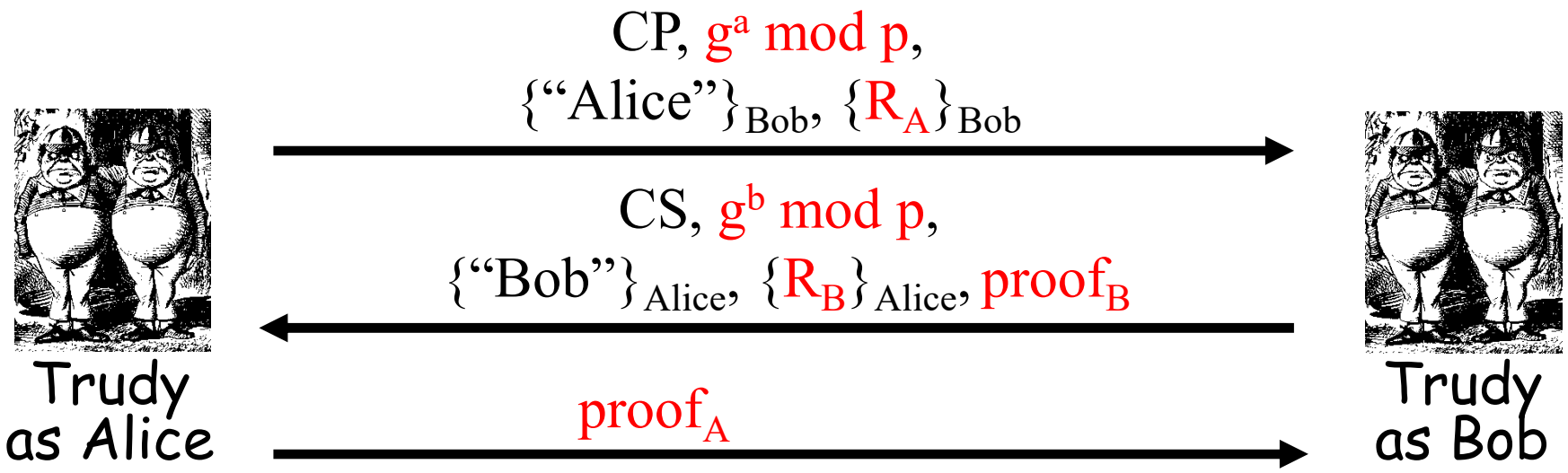


- K, $proof_A$, $proof_B$ computed as in main mode
- Note that identities are hidden
  - The only aggressive mode to hide identities
  - Then why have main mode?

Public Key Encryption Issue?

- Public key encryption, aggressive mode
- Suppose **Trudy** generates
  - Exponents **a** and **b**
  - Nonces $\mathbf{R_A}$ and $\mathbf{R_B}$
- Trudy can compute "valid" keys and proofs: $\mathbf{g^{ab}\ mod\ p}$, **K**, **SKEYID**, $\mathbf{proof_A}$ and $\mathbf{proof_B}$
- Also true of main mode

Public Key Encryption Issue?



- Trudy can create exchange that appears to be between Alice and Bob
- Appears valid to any observer, **including Alice and Bob!**

Plausible Deniability

- A security failure?
- In this mode of IPSec, it is a feature!
  - **Plausible deniability:** Alice and Bob can deny that any conversation has taken place!
- In some cases it might be a security failure
  - If Alice makes a purchase from Bob, she could later repudiate it (unless she had signed)

Summary

- **SSL**
- **IPSec**